

Architectures for Detecting Service Intruders and Holding Them Accountable Without Sacrificing User Privacy

Ulrich Flegel

Chair 6 · Information Systems and Security
Computer Science Department
University of Dortmund

Web Service Security Conference
May 26, 2006

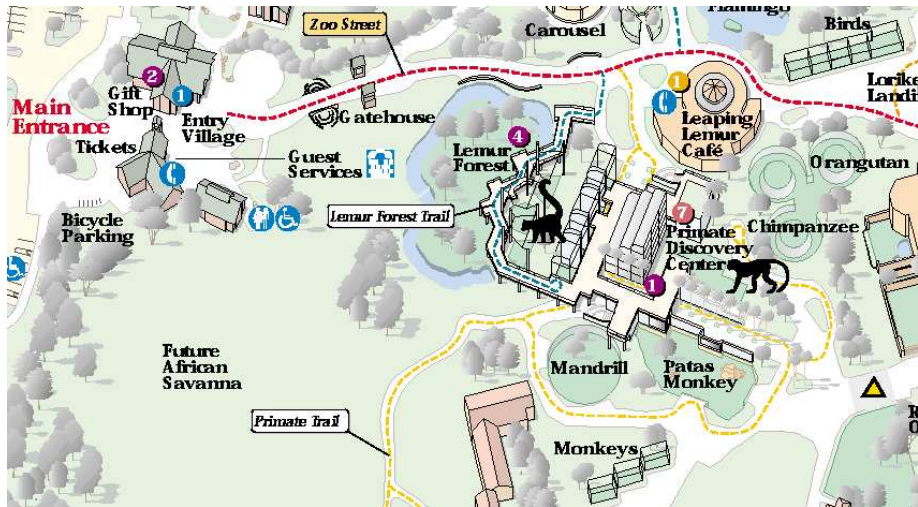


Overview

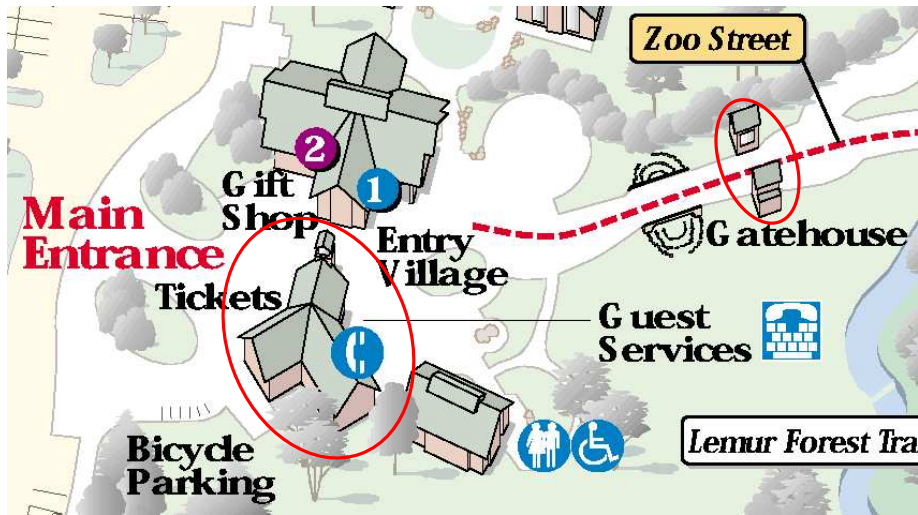
- 1 Authorizations
- 2 Architectural Model for Secure Authorizations
- 3 Misuse Detection
- 4 Privacy Issues
- 5 Architectural Model with Pseudonyms
- 6 Comparing Architectures
- 7 Example Architectures
- 8 Results



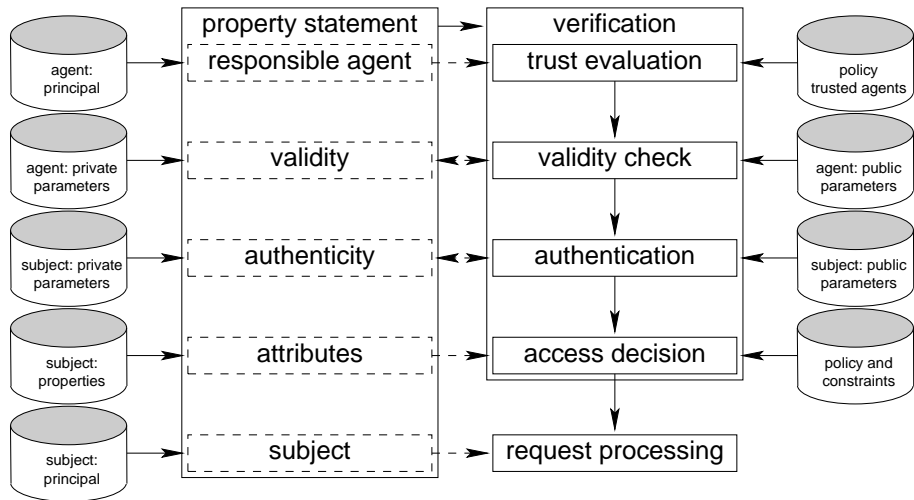
Visiting the Zoo



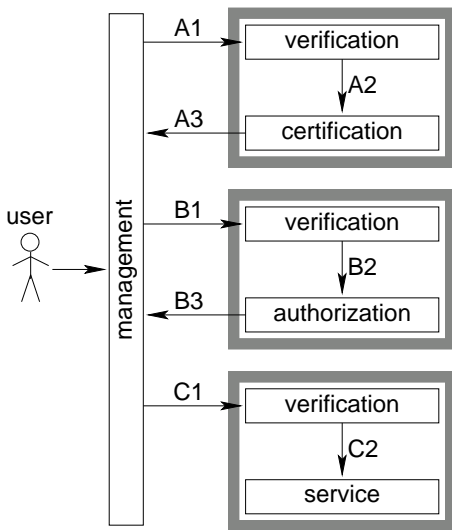
Ticket Booth and Entrance — Authorization



Verification of Property Statements



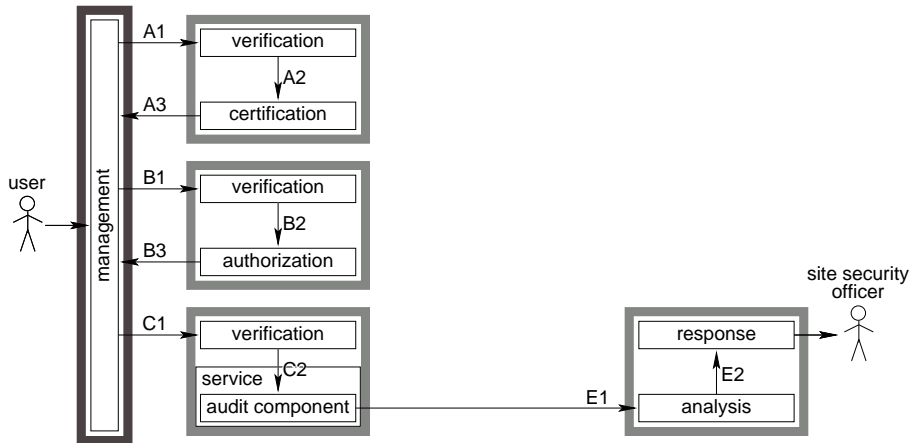
Basic Model



Zoo Guard — Misuse Detection



Focus: Audit Data Analysis Located at Service



Working Principle of Misuse Detection

Input: Audit Data

(=Log Data)

- accountable **usage data**
- documents service / system events incl. **user activity**

▶ example

▶ example

Working Principle of Misuse Detection

analyzing audit data requires the **linkability** of certain features in order to

- detect misuse
- asses the damage → remediate
- assess the exploited vulnerabilities → patch

Working Principle of Misuse Response

responding requires **accountability** of certain features in order to

- confine damage
- litigate

Conflicting Interests w.r.t. Misuse Detection

Relevance for Privacy

- audit data contains **personal data** ▶ example
- potentially affects **all users**: ▶ duality
performance monitoring, activity analysis, person profiling

Privacy Requirements

user expectations: individual anonymity ▶ expectations

user rights: informational self-determination ▶ rights

employee rights: co-determination w.r.t. perf. monitoring

data controller obligations: jungle of laws ▶ obligations

Misuse Detection in Practice

highly complex technical and statutory situation

⇒ intricacy of law-abiding solutions

Objective and Traditional Approach

Objective

fair balance between interests w.r.t.
privacy and misuse detection / response

▶ multilateral security

Traditional Approach: Pseudonyms

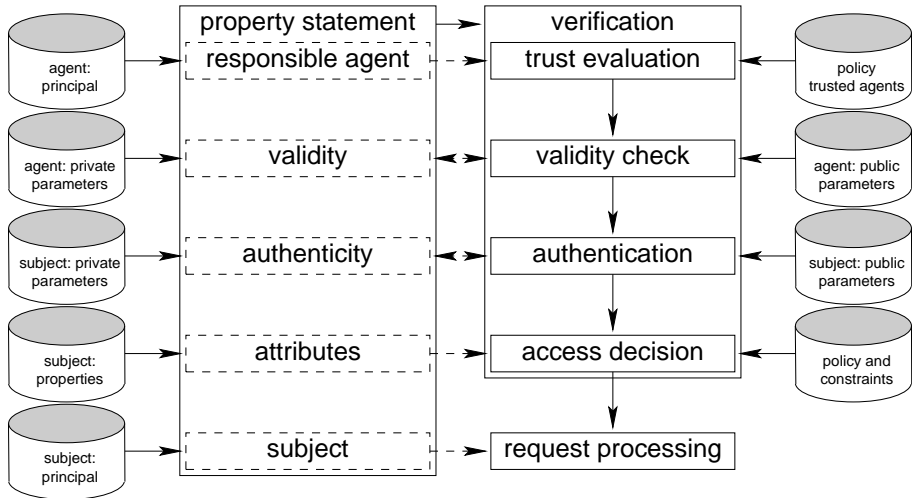
▶ terminology

- **replace personal data with pseudonyms**
- the **pseudonym mapping** associates pseudonyms with personal data and enables **pseudonym disclosure** ▶ examples
- **security** by controlling knowledge about the pseudonym mapping
- **fairness** by distinguishing between ▶ details ▶ key assumption

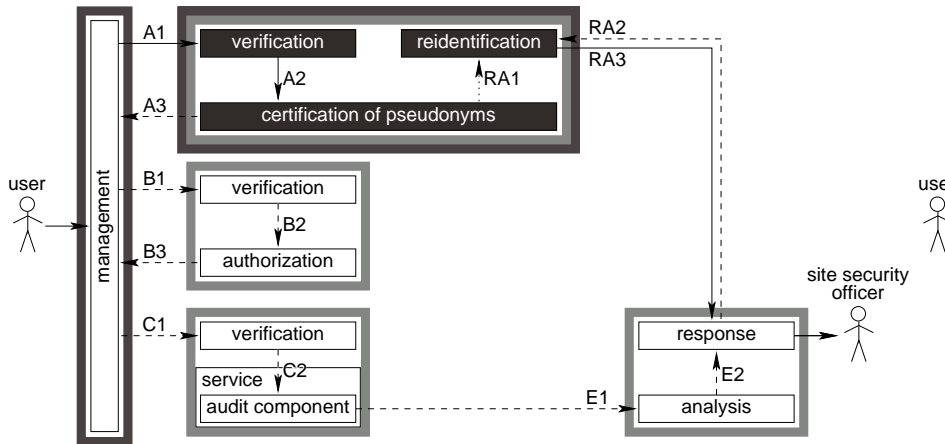
standard case: **no accountability**, pseudonyms cannot be disclosed
exceptional case: enable **accountability** by disclosing pseudonyms



Pseudonyms in Property Statements

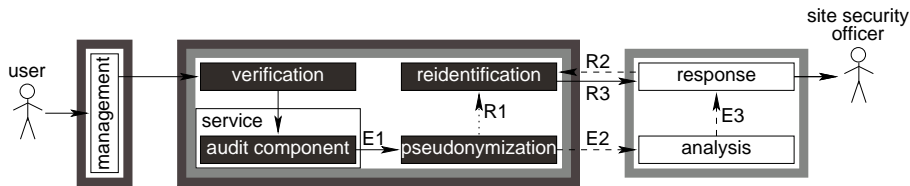


Introducing Pseudonyms in the Architectural Model

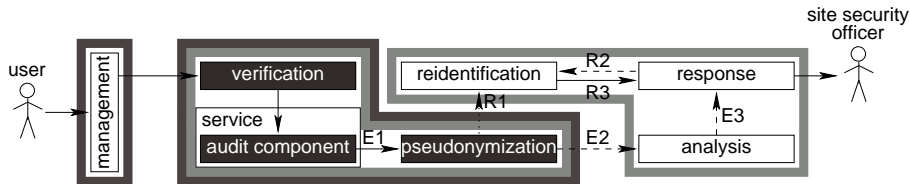


Purpose Binding

organizational vs. technical



Organizational purpose binding



Technical purpose binding



Comparing Architectures

property criteria	pseudonymizing entity			
	management	certifier	authorizer	service
privacy and accountability	–	✓	✓	✓
independence of service	✓	✓	–	–
dependable attributes	–	✓	✓	%
technical purpose binding	–	–	✓	✓
verifiability of pseudonyms b.a.	✓	✓	✓	–
independence of user	–	–	–	✓
independence of infrastructure	✓	–	–	✓



Example Architectures

Management

- privacy-enhanced **identity management**-client, e.g. using P3P

Certifier

- anonymous electronic **credentials** with anonymous authentication
- fair electronic offline **coins**

Authorizer

- anonymous electronic **tickets**
- **user account** under pseudonym

Service

- audit data **pseudonymizer**

Results for the Architectural Model

- architectures for secure (and pseudonymous) authorizations can be modeled
- **properties** of architectures can be derived and compared
- purpose binding of pseudonym disclosure can be enforced **technically** → **fair balance of security objectives**
- importance of suitable choice of **control requirements** and **crypto primitives**

Advantages of Direct Audit Data Pseudonymization

sole architecture simultaneously allowing

- **technical purpose binding** of pseudonym **disclosure**
- **short-term** and **cost-efficient** deployment

Contact

Ulrich Flegel

Dr. rer. nat

University of Dortmund
Computer Science Department
Chair 6
Informations Systems and Security
D-44221 Dortmund
Germany

+49 231 755 4775

`ulrich.flegel@udo.edu`

`http://ls6-www.cs.uni-dortmund.de/~flegel`

